REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application. The method claims are amended to conform to the new requirement that they be tied to another statutory class. At page 5, lines 22-28 of the applicants' specification, the applicants identify a number of machines/devices that could be configured with this invention. No new matter is added, and the intended scope of the claims is unchanged.

The applicants thank the Examiner for determining that claims 5-8 comprise patentable subject matter.

The Office action objects to the claims for the lack of indented elements. The claims are correspondingly amended herein.

The Office action rejects claim 17 under 35 U.S.C. 101. Claim 17 is correspondingly amended herein. Reconsideration of this rejection is respectfully requested.

The Office action provisionally rejects claim 1 on the ground of nonstatutory obviousness-type double patenting over claim 1 of U.S. patent application[1] 11/576,354. The applicants respectfully traverse this rejection.

Claim 1 of application 11/576,354 does not include a method wherein a first party additionally holds a value q_1 and a symmetrical polynomial $Q(x, z)$ fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, as specifically claimed in claim 1.

[1] The Office action refers to "U.S. Patent No. 11,576,354". In this response, the applicants assume that the Examiner intended to refer to U.S. patent application 11/576,354.

The Office action fails to identify where claim 1 of application 11/576,354 includes this feature, and merely states that claim 1 of application 11/576,354 claims pre-distributing a unique identifier based on "a master polynomial". Claim 1 of application 11/576,354 does not include a product of polynomials, and particularly does not include a product of two symmetric polynomials as claimed in claim 1 of this application.

Because claim 1 of application 11/576,354 does not claim each of the features of claim 1 of this application, the applicants respectfully maintain that the provisional double-patenting rejection of claim 1 over application 11/576,354 is unfounded, and should be withdrawn.

The Office action rejects claims 1, 9-12, and 16-19 under 35 U.S.C. 103(a) over Herzberg et al. (USP 5,202,921, hereinafter Herzberg) in view of Hoffstein et al. (USP 6,076,163, hereinafter Hoffstein). The applicants respectfully traverse this rejection.

The Office action acknowledges that Herzberg fails to teach a method wherein a first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, as specifically claimed in claim 1, upon which claims 2-15 depend, and relies on Hoffstein for providing this teaching. Claims 16-20 include similar features.

The Office action asserts that Hoffstein discloses "generating a secret key based on the product of two symmetrical polynomials" at column 3, lines 31-46 and FIG. 3. This assertion is incorrect. At the cited text, Hoffstein states:

> "The above-described user identification technique can be converted to a digital signature technique by the prover applying a one-way hash function to $A_g(x)$ and a message m to generate a simulated challenge polynomial c(x) which may be used in conjunction with g(x) and f(x) to generate the response polynomial h(x). The verifier receives m, $A_g(x)$ and h(x), uses the one-way hash function to derive c(x), and compares $A_h(x)$ to $A_g(x)*(A_f(x)+A_c(x))$ in order to authenticate the digital signature of the prover. Alternatively, the signature might consist of c(x) and h(x). From this $A_g(x)$ can be recovered as $A_h(x)*(A_f(x)+A_c(x))-1$ and the hash of this quantity and the message m can be compared to the polynomial c(x). A desired security level in both the user identification and digital signature techniques may be provided by selecting appropriate constraints for the polynomials g(x), c(x) and h(x)." (Hoffstein, column 3, lines 31-46.)

As is clearly evident, the cited text does not disclose a product of symmetrical polynomials, as specifically claimed in each of the applicants' independent claims. Of particular note, the term 'symmetrical polynomial' does not appear anywhere within Hoffstein.

Because the combination of Herzberg and Hoffstein fails to teach or suggest a method wherein a first party additionally holds a value q_1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q_1, and further performs the steps of sending q_1 to the second party, receiving a value q_2 from the second party and calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, the applicants respectfully maintain that the rejection of claims 1, 9-12, and 16-19 under 35 U.S.C. 103(a) over Herzberg and Hoffstein is unfounded, and should be withdrawn.

The Office action rejects:

claims 2-4 and 20 under 35 U.S.C. 103(a) over Herzberg in view of Hoffstein, and further in view of Matyes et al. (USP 5,953,420, hereinafter Matyes); and

claims 13-15 under 35 U.S.C. 103(a) over Herzberg in view of Hoffstein, and further in view of Menezes et al. (Handbook of Applied Cryptography, hereinafter Menezes). The applicants respectfully traverse these rejection.

Each of claims 2-4, 13-15, and 20 is dependent upon claim 1 or claim 16, and in these rejection, the Office action relies on the combination of Herzberg and Hoffstein for teaching the elements of claims 1 and 16. As noted above, the combination of Herzberg and Hoffstein fails to teach the elements of claims 1 and 16. The addition of Matyes and/or Menezes does not cure this deficiency with regard to claims 1 and 16. Accordingly, the applicants respectfully maintain that the rejections of claims 2-4, 13-15, and 20 under 35 U.S.C. 103(a) that rely on the combination of Herzberg and Hoffstein for teaching the elements of claims 1 and 16 is unfounded, and should be withdrawn.

In view of the foregoing, the applicants respectfully request that the Examiner withdraw the objection(s) and/or rejection(s) of record, allow all the pending claims, and find the application in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Reg. 41,508
804-493-0707
for: Kevin C. Ecker
Reg. 43,600

Please direct all correspondence to:
Corporate Counsel – IP&S
U.S. PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
914-332-0222